UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/809,073	03/16/2001	Lee Codel Lawson Tarbotton	00.164.01	5551

7590 06/27/2007

Zilka-Kotab, PC
P.O.Box 721120
San Jose, CA 95172-1120

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
06/27/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/809,073
Filing Date: March 16, 2001
Appellant(s): TARBOTTON ET AL.

Kevin Zilka
Registration No. 41,429
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 2/20/2007 appealing from the Office action mailed 9/12/2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal. Appellant mentions a prior appeal on p. 4 of the Appeal Brief, however it is clarified that this mentioned appeal was an appeal in the instant application.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is substantially correct. The changes are as follows:

WITHDRAWN REJECTIONS

The following grounds of rejection are not presented for review on appeal because they have been withdrawn by the examiner: **Claims 10, 24 & 38** under 35 U.S.C. 103(a) as being unpatentable over Kephart, Szor, Simpson and Davis, **Claims 12, 26 & 40** under 35 U.S.C.

103(a) as being unpatentable over Kephart and Symantec and **Claim 46** under 35 U.S.C. 103(a) as being unpatentable over Kephart and Golds.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

5,452,442	KEPHART	9-1995
6,694,434	MCGEE et al.	2-2004
6,216,112	FULLER et al.	4-2001
5,859,968	BROWN et al.	1-1999

Szor, Peter. "Bad IDEA", April 1998, Virus Bulletin, pp. 18-19.

Simpson, Sarah. "Cryptography In Everyday Life", 1997.

Veldman, Franz. "Heuristic Anti-Virus Technology", 1994, <http://www.madchat.org/vxdevl/papers/avers/heuris.txt>.

Symantec Corporation. "Norton AntiVirus User's Guide", 2000.

Lavasoft. "Ad-aware", February 2001.

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Based on Appellant's persuasive arguments, as further elaborated below, the rejections of claims 10, 12, 24, 26, 38, 40 & 46 have been withdrawn.

As such, claims 10, 12, 24, 26, 38, 40 & 46 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim Rejections - 35 USC § 102

1. Claims 1, 4, 7, 13, 15, 18, 21, 27, 29, 32, 35, 41 & 45 are rejected under 35 U.S.C. 102(b) as anticipated by or, in the alternative, under 35 U.S.C. 103(a) as obvious over U.S. Patent 5,452,442 to **Kephart**.

Regarding claims 1, 4, 7, 13, 15, 18, 21, 27, 29, 32, 35 & 41, Kephart discloses a user controlled program specifying logic (col. 5, lines 57-61) to specify said at least one computer program to be banned from use (col. 1, lines 35-49 & col. 5, lines 57-61), said at least one computer program comprising an undesired, non-virus computer program (col. 1, lines 15-34), and banned program identifying data generating logic responsive to said user controlled program specifying logic to generate banned program identifying data (signature, col. 5, lines 57-61) for at least one computer program to be banned from use, said banned program identifying data being operable to control anti computer virus logic (scanner, col. 1, lines 35-49) to identify computer programs banned from use (signatures are used in a virus scanner, col. 1, lines 35-49 & col. 2, lines 5-12). While Kephart is silent regarding the order of identifying computer viruses and programs banned from use, it is an inherent feature of Kephart's invention (a computer program) that, if the product/apparatus/method of Kephart is executed more than once, as is common in the art, regardless of whether viruses or non-viruses are identified first on the first execution, the second execution will have identified non-viruses after viruses because it identifies both each time. Further, if the ordering is not considered an inherent feature, one having ordinary skill in the art would have been motivated to modify Kephart in such a way that the system identifies the non-viruses after the viruses. One of ordinary skill in the art would have been motivated to perform such a modification to eliminate the most severe or crucial threats (viruses) before the less severe threats (non-viruses).

Regarding claim 45, Kephart discloses the user supplying a file from which signatures are extracted (col. 5, lines 57-61). Therefore, it is an inherent feature of Kephart that each end user anti computer virus logic includes a different selected set of computer programs banned from use.

Claim Rejections - 35 USC § 103

2. Claims 2, 8, 16, 22, 30 & 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Kephart**, as applied to claims 1, 7, 15, 21, 29 & 35 above, in further view of "Bad IDEA" by Peter Szor (**Szor**), in further view of "Cryptography in Everyday Life" by Sarah Simpson (**Simpson**). Kephart lacks encrypting the banned program identifying data (signatures) with a private key. However, Szor teaches that to prevent modification of antivirus signature files, the files should be encrypted (p. 19, col. 2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Kephart to encrypt the banned program identifying data (signatures). One of ordinary skill in the art would have been motivated to perform such a modification to prevent modification of antivirus signature files, as taught by Szor (p. 19, col. 2). As modified, Symantec lacks using a private key. However, Simpson teaches that by encrypting a file with a private key, the sender of the encrypted file can

be verified by decrypting it with the corresponding public key (p. 1, ¶1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a private key. One of ordinary skill in the art would have been motivated to perform such a modification to verify the creator of the signature files, as taught by Simpson (p. 1).

3. Claims 5, 19 & 33, are rejected under 35 U.S.C. 103(a) as being unpatentable over **Kephart**, as applied to claims 4, 18 & 32 above, in further view of "Heuristic Anti-Virus Technology" by **Veldman**. Kephart discloses detecting known viruses, but lacks the banned program identifying data including heuristic data identifying one or more behavioral characteristics. However, Veldman teaches that using heuristics and examining behaviors of a program allows detection of unknown viruses (§1 & §2.1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to including in the identifying data, heuristic data identifying one or more behavioral characteristics. One of ordinary skill in the art would have been motivated to perform such a modification to detect unknown computer viruses, as taught by Veldman (§1, ¶1 & §2.1).

4. Claims 11, 25 & 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Kephart**, as applied to claims 7, 21 & 35 above, in view of "Norton AntiVirus User's Guide", by Symantec Corporation (**Symantec**).

Regarding claims 11, 25 & 39, Kephart, as modified above, lacks explicitly triggering a banned program action. However, Symantec teaches that it is known to alert a user for a response (pp. 39-40). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Kephart's scanner to trigger a banned program action such as deleting the banned computer program (p. 40). One of ordinary skill in the art would have been motivated to perform such a modification to allow the user to rid the computer of the virus if the repair is not successful, as taught by Symantec (pp. 39-40).

5. Claims 6, 14, 20, 28, 34 & 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Kephart**, as applied to claims 1, 7, 15, 21, 29 & 35 above, in view of U.S. Patent 6,694,434 to McGee et al. (**McGee**). Kephart lacks the banned program identifying data comprising data identifying permitted compute programs with all computer programs not matching a permitted computer program being identified as a computer program banned from use. However, McGee teaches that it would be desirable to control whether a calling application can execute on a processor, since unauthorized applications can be inadvertently downloaded onto a system (col. 2, lines 35-41). McGee further discloses that each calling application's unique application verification data is generated upon it's calling and compared to a list of authorized programs (col. 3, line 64 – col. 4, line 4). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Kephart so that the banned program identifying data comprising data identifying permitted compute programs with all computer programs not matching a permitted computer program being identified as a computer program banned from use. One of ordinary skill in the art would have been motivated to perform such a modification to protect a computer against inadvertently downloaded unauthorized programs, as taught by McGee (col. 2, lines 35-41 & col. 3, line 64 – col. 4, line 4).

6. Claim 43 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Kephart**, as applied to claim 1, in view of "Ad-aware" by **Lavasoft** and U.S. Patent 6,216,112 to Fuller et al. **(Fuller)**. Kephart lacks the non-virus computer program including at least one of a game and a data streaming program. However, Lavasoft teaches that it is known to detect and remove spyware and adware (p. 1) because spyware can, for example, change a user's system (p. 1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Kephart to include spyware (adware) in the signatures, allowing the anti-virus logic to delete the adware (spyware). One of ordinary skill in the art would have been motivated to perform such a modification because detecting and removing adware and spyware is known in the art as beneficial, as taught by Lavasoft (p. 1). As modified, Kephart lacks explicitly a data streaming program. However, Fuller teaches that it is known in the art to install adware in a computer system, where the adware contacts servers and downloads new advertisements (streams data) (abstract). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to further modify Kephart to use the anti-virus software to remove data streaming programs. One of ordinary skill in the art would have been motivated to perform such a modification because adware streams data, as taught by Fuller (abstract).

7. Claim 44 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Kephart**, **Lavasoft**, and **Fuller**, in further view of U.S. Patent 5,859,968 to Brown et al. (**Brown**). Regarding claim 44, Kephart, as modified above by Lavasoft and Fuller, lacks the non-virus programs further including games. However, Brown teaches that it is known for an employer to

prevent the addition of games onto an employee computer (col. 4, lines 10-12). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Kephart such that the non-virus computer programs further include games. One of ordinary skill in the art would have been motivated to perform such a modification to enable employers to prevent the addition of the games to employee computers, as taught by Brown (col. 4, lines 10-12).

(10) Response to Argument

Issue #1

Group #1: Claims 1, 4, 7, 15, 18, 21, 29, 32 & 35

Appellant (p. 12) argues that Kephart's disclosure fails to suggest identifying viruses prior to identifying the computer programs banned from use because Kephart discloses that the procedure starts with a list of candidate signatures. The following language is taken from claim 1:

> "A computer program product ... comprising: user controlled program specifying logic ..., banned program identifying data generating logic ... said banned program identifying data being operable to control anti computer virus logic to identify computer programs banned from use; wherein the anti computer virus logic identifies computer viruses prior to identifying the computer programs banned from use."

From the above, we see that the invention of the instant application creates the banned program identifying data, which in turn is used by an anti-virus program to identify computer programs banned from use. The last clause indicates that the anti-virus program (in operation) identifies computer viruses prior to identifying the computer programs banned from use. The

Kephart reference teaches a virus scanner that creates identification signatures for computer viruses and other undesirable software entities and uses the signatures accordingly (in a virus scanning program) to identify the viruses or undesirable software entities. Therefore, Kephart teaches discloses the process. Kephart is silent regarding the ordering of identification, i.e. whether, once the signatures for viruses and non-viruses are created and being used to scan, viruses are identified before or after computer programs banned from use. It is noted that the claim language does not specify that all viruses be identified prior to identifying the computer programs. It is further noted that the claim does not recite scanning for viruses before scanning for non-viruses; rather the claim(s) recite(s) the outcome of the scanning such that viruses will be identified before non-viruses. The claim was rejected under 35 U.S.C. §102(b), or alternatively under 35 U.S.C. §103(a) (see p. 6 of the Office Action dated 9/12/2006).

102(b) argument: An initial interpretation of the Kephart reference suggests that when scanning, the reference will either identify a virus first or identify a non-virus first. However, because it is an inherent feature of Kephart's invention that both signatures for viruses and non-viruses are created and used for scanning, upon any subsequent execution/scanning (for which is software virus scanning is used), a non-virus will be identified after a virus. Therefore, because Appellant claims the outcome, the Examiner made an inherency argument regarding how this outcome would be necessarily achieved if the Kephart invention was put into practice, by scanning a subsequent time using the signatures created for both viruses and non-viruses.

103(a) argument: As an initial note, Appellant argues (p. 14, 2nd full ¶):

> "In addition, in the Office Action mailed 9/12/2006, the Examiner has argued that "one of ordinary skill in the art would have been motivated to prioritize the identification of viruses before identifying the computer programs banned from use because it is well known to identify the most severe threats first". First, it

> appears that, by incorporating an obviousness-type argument, the Examiner is improperly applying the prima facie case of obviousness in the context of a rejection under 35 U.S.C. 102(b)."

However, as stated above and clearly in the rejection of §11 of the Office Action dated 9/12/2006, the Examiner has rejected the claims over 102(b) or in the alternative, under 103(a) as obvious. As such, if the feature is not seen as inherent, the Examiner submits that one having ordinary skill in the art would see it as common sense knowledge to cause a program which scans for both viruses an non-viruses to specifically scan for viruses first to identify virus threats before non-virus threats. Again, Kephart teaches the process of creating signatures for viruses and non-viruses, but not the ordering of the identification. Viruses, as noted in the file history, are self-replicating meaning that they "spread" to different files or computer in a similar fashion to biological viruses spreading. Further, viruses are often destructive. The non-viruses noted by Kephart are for example Trojans, which are passive threats. Therefore, one having ordinary skill in the art understands that because viruses "get worse" over time, i.e. spread, and a more destructive, viruses are clearly more threatening to a system than non-viruses. As such, one having ordinary skill would have found identifying viruses before non-viruses as an obvious modification of Kephart in view of what was common knowledge to those having ordinary skill in the art at the time the invention was made.

Group #2: Claims 13, 27 & 41

Appellant's brief (p. 15) argues that Kephart does not disclose "wherein said anti computer virus logic is executable as a separate instance solely to identify computer programs banned from use." However, this limitation is further defining the outcome (i.e. the identification of non-viruses) of the Appellant's invention, such that at some point, only a non-virus will be identified. The claim is claiming that while the invention generates signatures for both viruses and non-viruses and operates an anti-virus scanner to use the created signatures, it has the *ability* to operate such that only a non-virus is identified. Regarding the "separate instance" language, all computer programs are run in an instance; i.e. the computer instantiates the program code by allocating memory, assigning variables, etc. to the program. Therefore Kephart's scanner meets this limitation. As such, Kephart's invention meets the limitation of claims 13, 27 & 41 because it *scans* for both viruses and non-viruses and therefore is executable as its own instance and can solely to identify computer programs banned from use (non-viruses) if it finds only non-viruses. Appellant argues that the Examiner stated that Kephart identifies both each time in the previous Office Action. This is true if the files/data, etc. being scanned contain both viruses and non-viruses. If Appellant is claiming a feature of the invention is to *scan* only programs banned from use (non-viruses), than it is submitted that the claims under consideration in this section fail to further limit the parent claim and as such are unpatentable over a non-virus scanner such as the cited Lavasoft reference which scans files for undesirable, but non-virus, software.

Group #3: Claim 45

Appellant's brief (p. 16) argues that Kephart fails to disclose "wherein the anti computer virus logic of a plurality of end users each includes a different selected set of computer programs banned from use." However, as seen in col. 5, lines 57-61, each user of Kephart's invention submits files containing a list of signatures or one or more files, each containing one or more portions of invariant viral code. Therefore, since the viruses and non-viruses for which Kephart's invention scans relies upon the user, it is absolutely inherent that all users will not submit the same data. Therefore, it is an inherent feature of Kephart that the virus logic used by Kephart's users will comprise a different set of programs to be banned from use.

Issue #2

Group #1: Claims 1, 4, 7, 15, 18, 21, 29, 32 & 35

Appellant's brief (pp. 17-20) argues similarly to the above-addressed arguments regarding the 102(b) and 103(a) rejections in view of Kephart. As such, the Examiner relies on the above responses to Appellant's arguments against claims 1, 4, 7, 15, 18, 21, 29, 32 & 35.

Group #2: Claims 13, 27 & 41

Appellant's brief (pp. 21-22) argues similarly to the above-addressed arguments regarding the rejections in view of Kephart. As such, the Examiner relies on the above responses to Appellant's arguments against claims 13, 27 & 41.

Group #3: Claim 45

Appellant's brief (pp. 22-12) argues similarly to the above-addressed arguments regarding the rejections in view of Kephart. As such, the Examiner relies on the above responses to Appellant's arguments against claims 45.

Issue #3

Group #1: Claims 2, 8, 16, 22, 30 & 36

Appellant's brief (p. 23) relies on the above arguments given with Issues #1, Group #1 & Issue #2, Group #2. Accordingly, the Examiner relies on the above-given responses to these arguments.

Issue #4

Group #1: Claims 5, 19 & 33

Appellant's brief (p. 23, regarding claims 5, 19 & 33) argues that Veldman fails to disclose the following limitation:

> "wherein said banned program identifying data includes heuristic data identifying at least one behavioral characteristic of at least one computer program banned from use such that variants of said at least one computer program banned from use that share said behavioral characteristics may also be identified."

Specifically Appellant argues that "suggesting the use of heuristics to detect instructions indicative of a virus, as in Veldman, simply fails to suggest that the "banned program identifying data **includes** heuristic data identifying at least one behavioral characteristic" (emphasis added)". However, as stated in the rejection, Kephart discloses detecting known viruses and other unwanted structures, such as Trojans (non-viruses), but lacks the details of the type of methods used to compare the files (actually determine correlation between the virus and the signature or the non-virus and the signature). However, Veldman teaches that using heuristics (generic detection) such that an examination the behaviors of a program allows the detection of unknown viruses. The basic idea is that when scanning for a virus, a specific virus detector will look for an exact signature – such that the virus will only be detected if it exists in the exact form known to the signature. On the other hand, heuristic virus scanning will look at the behavior of the program to determine if it is a virus. Consider the example where the virus file is renamed. In this case the specific virus scanner may not consider the file to be a virus. However, a heuristic scanner would be able to determine the file was a virus based on how it is executing, regardless of its name. Regarding the claim language, Appellant argues that Veldman cannot be applied to the virus scanner of Kephart. However, Kephart uses the same virus scanning engine for both viruses and non-viruses. Therefore, a scanning method used for one necessarily can be used for another. As such, since motivation is taught in Veldman for using heuristic detection methods to detect viruses, clearly one having ordinary skill in the art at the time the invention was made would have been motivated to apply the heuristic detection methods to the non-virus programs. The benefit gained is that the scanner cannot be circumvented by changing superficial characteristics of the non-virus program because the scanner looks at heuristics (behavior).

Issue #5

Group #1: Claims 10, 24 & 38

Appellant's brief (pp. 24-27) argues that it would not have been obvious to combine the teachings of Davis with the Kephart, Szor and Simpson references.

Appellant's arguments are persuasive and therefore the rejection is withdrawn.

Issue #6

Group #1: Claims 11, 25 & 39

Appellant's brief (pp. 24-27) argues that the excerpt from Symantec fails to suggest "wherein when a banned computer program is identified, at least one banned program action is triggered". Appellant further argues that "finding a virus that has infected a file, as in Symantec, teaches away from appellant's 'banned computer program' which 'comprises a non-virus computer program'". However, Symantec teaches a scanner looking for viruses; when a virus is detected, an action is taken. Kephart teaches a scanner looking for viruses and other non-virus programs, but lacks an action being taken. Clearly one having ordinary skill in the art at the time the invention was made would appreciate the benefit of taking one or more of the actions taught in Symantec when either of a virus or non-virus is found, such as deleting the banned program. The scanning in Kephart is evidence that the non-virus program, for example the Trojan disclosed in Kephart, is undesired and an action, such as for example the deleting of the identified file in Symantec, would be appropriate upon such identification.

Group #2: Claims 12, 26 & 40

Appellant's brief (pp. 27-28) argues that Symantec's downloading virus signatures from LiveUpdate fail to meet the limitation that the system is responding to "**an absence** of said **user generated** banned program identifying data". Upon review, the user of the Symantec program has no way of creating his/her own signatures and neither Symantec or Kephart discloses delivering signatures created by a user to a remote update server (such as LiveUpdate),

Appellant's argument is persuasive. Therefore, the rejection is withdrawn.

Issue #7

Group #1: Claims 6, 14, 20, 28, 34 & 42

Appellant's brief (p. 30) argues that McGee's "allowable application list" cannot render obvious the claimed "wherein said banned program identifying data comprises data identifying permitted computer programs with all computer programs not matching a permitted computer program being identified as a computer program banned from use" because McGee is non-analogous art directed to controlling program execution. However, the Examiner respectfully submits that Kephart is analogous art to McGee such that Kephart is dealing exactly with program execution. Kephart checks signatures to determine if a program is a virus (this type of conditional checking is sometimes referred to as a blacklist). McGee teaches an analogous concept (sometimes referred to as a whitelist), where all programs are considered threats (note that McGee even mentions viruses, see col. 2, lines 45-60) except programs matching an approved "signature" (McGee calls this a list of pre-approved hash values). It is commonly known that using a blacklist is common when most "items" to be matched to the list will be allowed, whereas it is commonly known to use a whitelist when most "items" to be matched to the list will be denied. For example, if there are only 10 programs "allowed" and all others are to be denied, a whitelist would be used because only a 10-element list would need to be checked as opposed to a potentially infinite list of "denied" elements. Conversely, if there are many programs allowed, it would take less time to search the smaller "denied" list than the entire "allowed" list. As such, it is submitted that it would have been obvious to one having ordinary skill in the art to use Kephart's virus/non-virus scanning program to create the list of "pre-approved hash values" (i.e. program signatures) disclosed in McGee. Again, Kephart and McGee are both dealing exactly with stopping the execution of unwanted programs. The advantage of this modification would be to protect the computer against inadvertently downloaded unauthorized programs, as taught by McGee (see col. 2, lines 35-41 & col. 3, line 64 – col. 4, line 4).

Issue #8

Group #1: Claim 43

Appellant's brief (p. 31) argues that there is no motivation to combine Fuller with Kephart. It is first noted, that Appellant makes no mention of the Lavasoft reference. However, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). In the instant situation, Appellant argues that Fuller and Kephart are non-analogous. However, as seen from the rejection, Kephart is directed to detecting undesirable programs (viruses and non-virus programs such as Trojans, etc.), but lacks the non-virus programs being specifically a data-streaming application. The Lavasoft reference teaches that it is known to detect "spyware" or "adware" on a computer that have been installed without the user's knowledge of it because spyware/adware can alter the user's system (p. 1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Kephart such that in addition or as an alternative to Trojans, spyware/adware programs are included in the non-virus, undesirable programs that Kephart seeks to identify. This would allow the benefit (taught by Lavasoft) of adware/spyware removal. While Lavasoft teaches adware/spyware, Lavasoft is silent as to the fact that adware/spyware can be data-streaming applications. However, Fuller is cited for teaching exactly that. Fuller discloses that adware in computer programs streams advertisements to a user's computer. Thus, Fuller is cited for teaching that one form of adware (which Kephart, as modified by Lavasoft seeks to identify and remove) is data-streaming applications (note that the name adware is derived from the fact that advertisements are downloaded/streamed to the user's computer). As such, it would have been obvious to include data-streaming applications within the scope of the non-virus programs that Kephart, as modified by Lavasoft, seeks to remove. This is because many adware programs are data-streaming applications (Fuller) and it is desirable to identify adware and remove it (Lavasoft).

Issue #9

Group #1: Claim 44

Appellant's brief (p. 32) argues that it would not have been obvious to combine Kephart and Brown. Specifically, Appellant argues that Kephart and Brown are not analogous art. Similarly to Issue #7, Appellant makes no mention of the Lavasoft and in this case also makes no mention of the Fuller reference in addressing the rejection. Again it is noted that one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Kephart is directed to detecting undesirable programs (viruses and non-virus programs such as Trojans, etc.). The Lavasoft reference teaches that it is known to detect "spyware" or "adware" on a computer that have been installed without the user's knowledge of it because spyware/adware can alter the user's system (p. 1). And Fuller is cited to teach that adware is often found in the form of data-streaming applications. Appellant's claim 44 seeks to include games as a non-virus program as it is used by the invention. For this, the Brown reference is cited. Kephart provides a means for determining a program is undesired, creating an anti-virus signature for the program, and using the anti-virus signature in anti-virus software (which uses the signature to detect a virus in another program and take action). Kephart is silent regarding whether the non-virus, undesired programs recited can include games. However, the Brown reference teaches that it is known for an employer to "prevent the addition of employer computer software, such as games, onto [a] computer". As Kephart's system is designed to prevent the addition of software and data deemed undesirable, it naturally flows from the references that one having ordinary skill in the art at the time the invention was made would have found it obvious to include games in the category of undesirable, non-virus software to be identified by Kephart. The motivation is taken directly from Brown such that it is known for an employer to want to prevent employees from playing games. Appellant argues that, because Brown achieves this result differently then does Kephart, the arts are non-analogous. However, Kephart provides the necessary tools to designate undesirable software to be identified as undesirable by a virus scanner. Brown is cited for teaching specifically that there is reason that this undesirable software be a game.

Issue #10

Group #1: Claim 46

Appellant's brief (p. 33) argues that Golds fails to teach "wherein an anti-virus scan is performed when a file access is received, and if said anti-virus scan is not passed, an anti-virus action is triggered and a fail response is returned to an operating system, and if said anti-virus scan is passed, a scan for the computer programs banned from use is performed".

This argument is persuasive. Accordingly, the rejection is withdrawn.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Michael J. Simitoski

/Michael J. Simitoski/

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER

Conferees:

Kim Vu KVu

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER

Kambiz Zand